IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

ROBERT PICON, individually and on behalf of all others similarly situated, Plaintiff, v. TRAVELEX CURRENCY SERVICES INC., Defendant.	Civil Action No.: 1:20-cv-03147-PKC **FIRST AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Robert Picon ("Plaintiff" or "Mr. Picon"), by and through his attorneys, makes the following allegations against Defendant Travelex Currency Services Inc. ("Defendant" or "Travelex") pursuant to the investigations of his counsel and upon information and belief, except as to the allegations specifically pertaining to himself or his counsel, which are based on personal knowledge.

NATURE OF THE ACTION AND FACTS COMMON TO ALL CLAIMS

1. Plaintiff brings this class action against Defendant for its failure to secure and safeguard his personal identifying information ("Personal Information"), and the Personal Information of hundreds of thousands of other current and former Travelex customers and employees.

2. Travelex is one of the world's largest foreign currency exchange companies, with currency exchange ATMs and branch locations at many of the world's biggest airports and cities. Travelex also allows customers to purchase a "Money Card" (formerly a "Cash Passport") that can be used in "millions of locations" around the world, despite differences in currency. Travelex operates 175 retail locations nationwide where United States customers are able to

exchange currency.[1]

3. Travelex's currency exchange ATMs and kiosks are ubiquitous in airports and major travel center across the United States:

4. Unfortunately for its customers and employees, in late 2019, Travelex experienced a massive data breach in which hackers accessed the Personal Information of its customers and employees (hereinafter, the "Data Breach"). The hack forced Travelex to take its internal networks, consumer-facing websites, and app offline for several weeks.

[1] https://www.travelex.com/sell-your-foreign-currency (last accessed April 16, 2020).

5. The hackers reportedly gained access to Travelex's entire computer network with access to all of its most sensitive information, including its customers and employees' Personal Information, and even obtained access to customers and employees' dates of birth, credit and debit card information, social security numbers, phone numbers, address information, and banking information.[2]

6. Indeed, the data breach was so severe that Travelex paid the hackers roughly $2.3 million in ransom.[3]

7. As set forth herein, the Data Breach was the inevitable result of Defendant's inadequate approach to data security and their failure to protect Class Members' Personal Information that they collected, maintained, and disseminated during the course of their business. While Travelex reportedly discovered the Data Breach on December 31, 2019, hackers had accessed and encrypted Personal Information months prior – potentially even as far back as the summer of 2019.[4] That means for perhaps as long as six months, hackers had unfettered accessed to Personal Information before Defendant took any steps to alleviate the hack. Further, Defendant was warned months prior to the hack that it was vulnerable to Sodinokibi ransomware, the very method of the hack, and yet Defendant waited months to fix critical flaws in its security systems.[5] Defendant's most recent hack and exposure of Personal Information is particularly glaring in light of the fact that Defendant had experienced a large data breach just years prior.

---

[2] https://www.bbc.com/news/business-51017852 (last accessed April 16, 2020).
[3] https://www.wsj.com/articles/travelex-paid-hackers-multimillion-dollar-ransom-before-hitting-new-obstacles-11586440800 (last accessed April 16, 2020).
[4] https://www.independent.co.uk/news/business/news/travelex-cyber-hack-data-breach-foreign-exchange-money-a9275736.html (last accessed April 16, 2020).
[5] https://www.independent.co.uk/news/business/news/travelex-cyber-hack-data-breach-foreign-exchange-money-a9275736.html (last accessed April 16, 2020).

8. At first, Defendant tried to hide the fact that hackers had gained access to Personal Information, or that a hack had occurred. Defendant initially declared that its global system outage was due to maintenance downtime via a message on its website.[6] A week later, Defendant finally announced that it had been the subject of a cyberattack.

9. Unfortunately for Plaintiff and Class Members, the ramifications of Defendant's failure to keep Plaintiff's and Class Members' data secure are severe. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R § 248.201. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person." *Id*.

10. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[7]

11. Identity thieves can use personal information, such as that of Plaintiff and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

---

[6] https://www.infosecurity-magazine.com/blogs/travelex-incident-changing/ (last accessed April 16, 2020).

[7] Federal Trade Commission, Warning Signs of Identity Theft (May 2015), available at https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited June 18, 2019).

12. Annual monetary losses from identity theft are in the billions of dollars.

According to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration. In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[8]

13. The unauthorized disclosure of Social Security Numbers can be particularly damaging because Social Security Numbers cannot easily be replaced. To obtain a new number, a person must prove, among other things, he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until the damage has been done. Furthermore, as the Social Security Administration warns:

> A new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit reporting companies use the number, along with other Personal Information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other Personal Information, such as your name and address, remains the same. If you receive a new Social Security Number, you will not

[8] Federal Trade Commission, Combating Identity Theft A Strategic Plan (April 2007) available at https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategicplan/strategicplan.pdf (last visited June 18, 2019).

> be able to use the old number anymore. For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit.[9]

14. Personal Information such as that stolen in the Data Breach is highly coveted by, and a frequent target of, hackers because thieves can use the credit card information to create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; thieves can reproduce stolen debit cards and use them to withdraw cash from ATMs; use the victim's Personal Information to commit immigration fraud, obtain a driver's license or identification card in the victim's name but with another's picture, use the victim's information to obtain government benefits, file a fraudulent tax return using the victim's information to obtain a fraudulent refund; get medical services using consumers' stolen information or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

15. Further, without detailed, prompt disclosure by Defendant to Plaintiff and Class Members who have been impacted, affected individuals, including Plaintiff and Class Members, will be left exposed, unknowingly and unwittingly, for potentially months to continued misuse and ongoing risk of misuse of their Personal Information without being able to take necessary precautions to prevent imminent harm.

16. And even those individuals who are reimbursed for a financial loss due to fraud are not made whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the

[9] Social Security Administration, Identity Theft and Your Social Security Number (June 2017), available at http://www.ssa.gov/pubs/10064.html (last visited June 18, 2019).

Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[10]

17. There may also be a time lag between when harm occurs versus when it is discovered, and also between when Personal Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[11]

18. Thus, Plaintiff and Class Members now face *years* of constant surveillance of their financial and personal records and will continue to spend time, effort, and money attempting to protect themselves from ongoing identity theft and fraud. To address these increased risks, they must incur, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft.

19. The Personal Information of Plaintiff and Class Members is private and sensitive in nature and was left inadequately protected by Defendants.

20. The Data Breach was a direct and proximate result of Defendant's failure to

[10] U.S. Department of Justice, Victims of Identity Theft, 2014 (Sept. 2015) available at http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited June 18, 2019).
[11] U.S. Government Accountability Office, Report to Congressional Requesters (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited June 18, 2019).

adequately monitor and audit the data security systems and its failure to properly safeguard and protect Plaintiff's and Class Members' Personal Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including its failure to establish, implement, and ensure appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' Personal Information to protect against reasonably foreseeable threats to the security or integrity of such information.

21. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach.

22. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' Personal Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation.

23. Defendant continues to hold Personal Information, including the Plaintiff's and Class Members' Personal Information, and, therefore, Plaintiff and the Class have an undeniable interest in ensuring that their Personal Information is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

24. Defendant's actions and omissions violate well-established legal and statutory duties they owed to Plaintiff and Class Members.

25. Plaintiff brings this action on behalf of himself and all others similarly situated for

actual damages, as well as punitive damages and equitable and injunctive relief to fully redress the widespread harm Defendant's wrongful acts and omissions have unleashed.

JURISDICTION AND VENUE

26. This Court has original jurisdiction over this controversy pursuant to 28 U.S.C § 1332(d) because there are more than 100 class members and the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interest, fees, and costs, and at least one Class member is a citizen of a state different from Defendant.

27. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) and (c) because the real property at issue is located in this District, and a substantial part of the events or omissions that give rise to this action occurred in this District.

PARTIES

28. Plaintiff Robert Picon is, and at all times mentioned herein was, a resident of San Francisco, California and a citizen of the State of California. Plaintiff used a Travelex kiosk in 2018 at an airport in California to exchange currency for a trip to Mexico. Accordingly, as a result of the transaction, Travelex obtained Personal Information regarding Mr. Picon, which was later stolen and put at risk during the Data Breach. The Data Breach and disclosure of the Personal Information has immediately, directly and substantially increased Mr. Picon's risk of identity theft. Indeed, information such as data breach victims' names, birth dates, social security numbers, and bank account numbers and other identifying information creates a material risk of identity theft. As a result of the Data Breach, Mr. Picon also has suffered a loss of privacy, nuisance and diminished value of Personal Information, and must now expend additional time and money mitigating the threat of identity theft that would not be necessary but for the Data Breach.

29. Defendant Travelex Currency Services Inc. is a Delaware corporation with its principal place of business at 355 Lexington Ave., New York, New York.

CLASS ACTION ALLEGATIONS

30. Plaintiff seeks relief in his individual capacity and as a representative of all others who are similarly situated. In accordance with Fed. R. Civ. P. 23(a) and (b)(2) and/or (b)(3), Plaintiff seeks certification of a Nationwide Class and a California subclass.

31. The Nationwide Class is defined as all persons residing in the United States whose personal information was disclosed in the Data Breach affecting Travelex (the "Class").

32. The California Class is defined as all persons residing in California whose personal information was disclosed in the Data Breach affecting Travelex (the "California Class").

33. Excluded from the Classes are Defendant; any of their corporate affiliates; any of their directors, officers, or employees; any persons who timely elects to be excluded from any of the Classes; any government entities; and any judge to whom this case is assigned and their immediate family and court staff.

34. The members of each Class are so numerous that the joinder of all members is impractical. The Class likely includes hundreds of thousands, if not millions of people.

35. Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Common legal and factual questions include, but are not limited to: (a) Whether Defendant had a legal duty to use reasonable security measures to protect Personal Information; (b) Whether Defendant was negligent in failing to protect the Personal Information of Plaintiff and the Class Members; (c) Whether Defendant was unjustly enriched by its failure to protect the Personal Information of Plaintiff and the Class

Members; (d) Whether Defendant violated California Business and Professions Code § 17200, *et seq.*; (e) Whether Defendant violated the Federal Trade Commission Act, 15 U.S.C. § 45; (f) whether Defendant violated the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, *et seq.*; and (g) The nature of the relief, including equitable relief and damages, to which Plaintiff and the Class Members are entitled.

36. Plaintiff's claims are typical of the claims of the members of the Classes, and Plaintiff will fairly and adequately protect the interests of the Classes. Plaintiff and all members of the Classes are similarly affected by Defendants' wrongful conduct in that their Personal Information has been exposed without their authorization.

37. Plaintiff's claims arise out of the same common course of conduct giving rise to the claims of the other members of the Classes.

38. Plaintiff's interests are coincident with, and not antagonistic to, those of the other members of the Classes.

39. Plaintiff is represented by counsel competent and experienced in the prosecution of consumer protection and tort litigation.

40. The questions of law and fact common to the members of the Classes predominate over any questions affecting only individual members, including legal and factual issues relating to liability and damages.

41. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Among other things, such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort and expense if numerous individual actions. The benefits of proceeding as a class, including providing injured persons or entities

with a method for obtaining redress for claims that might not be practicable to pursue individually, substantially outweigh any potential difficulties in managing this class action.

COUNT I
Violation Of The California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, *et seq.*
(On Behalf Of The California Class)

42. Plaintiff incorporates by reference the allegations in the preceding paragraphs as if fully set forth herein.

43. Plaintiff brings this count on behalf of himself and the California Class.

44. Defendant violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff's and California Class members' nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff and California Class members.

45. As a direct and proximate result of Defendant's acts, Plaintiff's and California Class members' PII was subjected to unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violation of the duty: through Defendant's internal networks, consumer-facing website, app, and ATM and kiosk network, and/or from the dark web, where hackers further disclosed ("as a result of [Defendant's] violation of the duty") Defendant's customers' PII in 2019 and after January 1, 2020.

46. As a direct and proximate result of Defendant's acts, Plaintiff and California Class members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of California Class members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as

described herein. Defendant's breach of its duties has directly and proximately injured Plaintiff and members of the California Class, including by foreseeably causing them to expend time and resources investigating the extent to which their Personal Information has been compromised, taking reasonable steps to minimize the extent to which the breach puts their credit, reputation, and finances at risk, and taking reasonable steps (now or in the future) to redress fraud, identity theft, physical, emotional, and mental harm of the data breach, and similarly foreseeable consequences of unauthorized and criminal access to their Personal Information.

47. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard California Class members' PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California Class members.

48. Defendant is a corporation that is organized or operated for the profit or financial benefit of its owners, with annual gross revenues over $25 million. Defendant collects consumers' PII as defined in Cal. Civ. Code § 1798.140.

49. Defendant failed to "actually cure" its violations of Cal. Civ. Code § 1798.150(a) within 30 days of Plaintiff's written notice to them that identified § 1798.150(a) as the specific provision of the CCPA that Defendant violated or are violating. *See* § 1798.150(b) ("Actions pursuant to [the CCPA] may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated."). Moreover, Defendant failed to provide "an express written statement that the violations have been cured and that no further violations shall occur,"

as required by § 1798.150. A copy of Plaintiff's letter is attached as Exhibit A.

50. Plaintiff and California Class members seek relief under § 1798.150(a), including, but not limited to, recovery of actual damages, or damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident, whichever is greater; injunctive or declaratory relief; any other relief the court deems proper; and attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5).

COUNT II
Negligence
(On Behalf Of The Class And California Class)

51. Plaintiff incorporates by reference the allegations in the preceding paragraphs as if fully set forth herein.

52. Plaintiff brings this count on behalf of himself, the Class, and the California Class.

53. Defendant owed a duty to Plaintiff and Class Members, who were required to provide their Personal Information to Defendant in connection with using its services. Defendant created a duty through its voluntary actions in collecting and storing the Personal Information for its own benefit, as well as by its assurances that it would safeguard that information.

54. Defendant's duty required it, among other things, to design and employ cybersecurity systems, anti-hacking technologies, and intrusion detection and reporting systems sufficient to protect Personal Information from unauthorized access and to promptly alert their users of data breaches.

55. Defendant breached its duties by, among other things: failing to maintain appropriate technological and other systems to prevent unauthorized access; failing to minimize

the Personal Information that any intrusion could compromise; failing to detect the Data Breach in a timely manner; failing to promptly notify Plaintiff and Class Members of the Data Breach.

56. Defendant's breaches of its duties provided the means for third parties to access, obtain, and misuse the Personal Information of Plaintiff and the Class without authorization. It was reasonably foreseeable that such breaches would expose the Personal Information to criminals and other unauthorized access.

57. But for Defendant's breach of its duties, Class Members' Personal Information would not have been compromised in the Data Breach.

58. As a result of Defendant's negligence, Plaintiff and the Class suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiff and class member must more closely monitor their financial accounts and credit histories to guard against identity theft and misuse of their Personal Information. Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized release of Plaintiff's and Class Members' Personal Information also diminished the value of that Personal Information.

59. The damages to Plaintiff and other Class Members were a proximate, reasonably foreseeable result of Defendant's breaches of their duties. Plaintiff and class member are entitled to damages in an amount to be proven at trial

COUNT III
Unjust Enrichment
(On Behalf Of The Class And The California Class)

60. Plaintiff incorporates by reference the allegations in the preceding paragraphs as

if fully set forth herein.

61. Plaintiff brings this count on behalf of himself, the Class, and the California Class.

62. Defendant knowingly and deliberately enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

63. Plaintiff and Class Members suffered and will continue to suffer injuries in the form of identity theft, attempted identity theft, the expense in mitigating harms, diminished value of Personal Information, loss of privacy, and nuisance.

64. Plaintiff, on behalf of himself and the Class Members, therefore seeks relief in the form of restitution.

COUNT IV
Violation Of California's Unfair Competition Law, Bus. & Prof. Code § 17200 *et seq*.
(On Behalf Of The Class)

65. Plaintiff incorporates by reference the allegations in the preceding paragraphs as if fully set forth herein.

66. Plaintiff brings this count on behalf of himself and the Class.

67. Defendant engaged in unfair, fraudulent and unlawful business practices in violation of the Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL").

68. Plaintiff and California Class Members suffered an injury in fact because of

Defendant's alleged violations of the UCL.

69. The acts, omissions, and conduct of Defendant as alleged constitute a "business practice" within the meaning of the UCL.

70. Defendant violated the unlawful prong of the UCL by violating the Federal Trade Commission Act, 15 U.S.C. § 45, as alleged herein.

71. Defendant violated the unlawful prong of the UCL by violating the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, *et seq.*, as alleged herein.

72. Defendant's acts, omissions, and conduct also violate the unfair prong of the UCL because they offended public policy and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff and other California Class Members. The harm cause by Defendant's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendant's legitimate business interests, other than Defendant's conduct described herein.

73. Defendant engaged in a fraudulent business practice that is likely to deceive a reasonable consumer by not having adequate measures to prevent data theft. A reasonable person would find Defendant's omissions material.

74. As a result of Defendant's violations of the UCL, Plaintiff and the other California Class Members are entitled to injunctive relief and restitution of all funds Defendant acquired as a result of their unfair competition.

COUNT V
Negligence *Per Se* For Violation of the Federal Trade Commission Act, 15 U.S.C. § 45
(On Behalf Of The Class And the California Class)

75. Plaintiff incorporates by reference the allegations in the preceding paragraphs as if fully set forth herein.

76. Plaintiff brings this count on behalf of himself, the Class, and the California Class.

77. Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce." The FTC has held that the failure to employ reasonable measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5.

78. The FTC has provided guidance on how businesses should protect against data breaches, including: protect the personal customer information they acquire; properly dispose of personal information that is not necessary to maintain; encrypt information stored on computer networks; understand their network's vulnerabilities; and install vendor-approved updates to address those vulnerabilities. FTC guidance also recommends that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating that someone may be trying to penetrate the system; and watch for large amounts of data being transmitted from the system.

79. Plaintiff and members of the Classes are within the Classes of persons Section 5 of the FTCA was intended to protect.

80. The harm that has occurred is the type of harm the FTCA was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and members of the Classes.

81. Defendant owed a duty to Plaintiff and members of the Classes under the Section 5 of the FTCA.

82. Defendant breached its duty under Section 5 of the FTCA by, among other things,

failing to maintain appropriate technological and other systems to prevent unauthorized access to its database, failing to properly design the database to avoid defects or other errors, and failing to provide timely notice to affected consumers with accurate information so that those affected could begin minimizing the impact of the incident.

83. Defendant's breach of its duties has directly and proximately injured Plaintiff and members of the Classes, including by foreseeably causing them to expend time and resources investigating the extent to which their Personal Information has been compromised, taking reasonable steps to minimize the extent to which the breach puts their credit, reputation, and finances at risk, and taking reasonable steps (now or in the future) to redress fraud, identity theft, physical, emotional, and mental harm of the data breach, and similarly foreseeable consequences of unauthorized and criminal access to their Personal Information.

84. Plaintiff and the members of the Classes are entitled to damages in an amount to be proven at trial, and to equitable relief, including injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands judgment on behalf of themselves and members of the Classes as follows:

A. For an order certifying the Class and/or California Class under Rule 23 of the Federal Rules of Civil Procedure; naming Plaintiff as Class and Subclass representative; and naming Plaintiff's attorneys as Class Counsel representing the Class and Subclass members;

B. For an order finding in favor of Plaintiff, the Class, and California Class on all counts asserted herein;

C. For an order awarding compensatory damages, statutory damages, and/or restitution in amounts to be determined by the Court and/or jury;

D. For an order awarding punitive damages where the Court deems proper;

E. For injunctive relief enjoining the illegals acts detailed herein;

F. For prejudgment interest on all amounts awarded;

G. For an order awarding Plaintiff their reasonable attorneys' fees and expenses and costs of suit; and

H. Such other or further relief as the Court may deem appropriate.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: June 23, 2020

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ Neal J. Deckant*
Neal J. Deckant

Neal J. Deckant (State Bar No. 5026208)
Yeremey Krivoshey (*pro hac vice* app. forthcoming)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-Mail: ndeckant@bursor.com

BURSOR & FISHER, P.A.
Scott A. Bursor (State Bar No. 2806487)
2665 S. Bayshore Dr., Suite 220
Miami, FL 33133-5402
Telephone: (305) 330-5512
Facsimile: (305) 676-9006
E-Mail: scott@bursor.com

Counsel for Plaintiff

EXHIBIT A

BURSOR & FISHER P.A.

1990 NORTH CALIFORNIA
BLVD. SUITE 940
WALNUT CREEK, CA 94596
www.bursor.com

NEAL J. DECKANT
Tel: 925.300.4455
Fax: 925.407.2700
ndeckant@bursor.com

April 17, 2020

Via Certified Mail – Return Receipt Request

Travelex Currency Services Inc.
355 Lexington Ave, 3rd Floor
New York, NY 10017

C T Corporation
28 Liberty St.
New York, NY 10005

Re: *Demand Letter Pursuant to the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100., et seq.; and all other state and local laws*

To Whom It May Concern:

This letter serves as a preliminary notice and demand for corrective action by Travelex Currency Services Inc. ("You" or "Travelex") pursuant to numerous provisions of California law, including the California Consumer Privacy Act, Cal. Civ Code. §§ 1798.100, *et seq.*, on behalf of our client, Robert Picon. This letter also serves as notice for claims of negligence and negligence *per se*. Mr. Picon is acting on behalf of himself as well as a class defined as all persons in the United States whose personal identifying information was maintained by Travelex that was compromised as a result of the data breach announced by You in December 2019/January 2020 (the "Data Breach"). Mr. Picon is also acting on behalf of himself as well as a class defined as all persons in California whose personal identifying information was maintained by Travelex that was compromised as a result of the breach announced by You in December 2019/January, 2020.

In late December 2019 and early January 2020, Travelex announced that hackers gained access to Travelex's entire computer network, with access to all of its most sensitive information, including its customers and employees' Personal Information, such as dates of birth, credit and debit card information, social security numbers, phone numbers, address information, and banking information. The Data Breach was the inevitable result of Your inadequate approach to data security and Your failure to protect Personal Information that You collected, maintained, and disseminated during the course of Your business. While Travelex reportedly discovered the Data Breach on December 31, 2019, hackers had accessed and encrypted Personal Information months prior – potentially even as far back as the summer of 2019. That means for perhaps as long as six months, hackers had unfettered accessed to Personal Information before You took any steps to alleviate the hack. Further, You were warned months prior to the hack that You were vulnerable to Sodinokibi ransomware, the very method of the hack, and yet You waited

months to fix critical flaws in Your security systems. Your most recent hack and exposure of Personal Information is particularly glaring in light of the fact that You experienced a large data breach just years prior. You failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, and to protect the personal information from unauthorized access, use, and disclosure. Because of these failure on Your part, customer and employee information has been compromised.

Our client, Robert Picon, is a resident of San Francisco, California. Mr. Picon used a Travelex kiosk in 2018 at an airport in California to exchange currency for a trip to Mexico. Accordingly, as a result of the transaction, Travelex obtained Personal Information regarding Mr. Picon, which was later stolen and put at risk during the Data Breach. The Data Breach and disclosure of the Personal Information has immediately, directly and substantially increased Mr. Picon's risk of identity theft.

Further, Mr. Picon seeks relief on behalf of a subclass of similarly situated California consumers under the California Consumer Privacy Act ("CCPA"), Cal. Civ Code. §§ 1798.100, *et seq*. Pursuant to the CCPA, "any consumer whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action." Cal. Civ. Code § 1798.150(a)(1). Here, as a result of Your failure to implement and maintain reasonable security procedures and practices, Mr. Picon's Personal Information was subject to unauthorized access and disclosure. Pursuant to the CCPA, Mr. Picon seeks statutory damages in an amount not less than one hundred dollars ($100), injunctive or declaratory relief, and any other relief the court deems proper. Cal. Civ. Code § 1798.150(a)(1)(A-C). This letter likewise serves as notice under the CCPA, pursuant to Cal. Civ. Code § 1798.150(b).

To cure these defects, we demand that you make full restitution to all persons for their time, expense, and injury of dealing with the data breach.

We further demand that you preserve all documents and other evidence which refer or relate to any of the above-described practices including, but not limited to, the following:

1. All documents concerning the design, development, testing, implementation, and/or maintenance of your security systems, including but not limited to your mobile application;

2. All documents concerning your knowledge of potential digital security incidents involving your systems, including the data breach that is the subject of this letter;

3. All documents concerning requests for personal identifying information from consumers;

4. All documents concerning your collection, storage, and use of the personal identifying information of consumers and employees;

5. All documents or communications concerning areas of exposure that may have resulted in the data breach;

6. All documents and communications with law enforcement concerning your response to the data breach; and

7. All documents or communications concerning the number of persons affected by the data breach, and lists of those persons.

If you contend that any statement in this letter is inaccurate in any respect, please provide us with your contentions and supporting documents immediately upon receipt of this letter.

Please contact me right away if you wish to discuss an appropriate way to remedy this matter. If I do not hear from you promptly, I will take that as an indication that you are not interested in doing so.

Very truly yours,

Neal J. Deckant